



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/905,113	07/16/2001	Scott A. Vanstone	06944.0044	3558

27155 7590 12/07/2004

MCCARTHY TETRAULT LLP  
SUITE 4900, P.O. BOX 48  
66 WELLINGTON ST. WEST  
TORONTO, ON M5K 1E6  
CANADA

EXAMINER

NORRIS, TREMAYNE M

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 12/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

**Application No.**

09/905,113

**Applicant(s)**

VANSTONE, SCOTT A.

**Examiner**

Tremayne M. Norris

**Art Unit**

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 16 July 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-12 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 16 July 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>2/27/03 ; 1/22/02</u> | 6) <input type="checkbox"/> Other: _____  |

## **DETAILED ACTION**

### ***Specification***

1. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.
2. The disclosure is objected to because of the following informalities: It is not clear what reference number 30 is. On page 6 line 24 and on page 7 line 18 reference number 30 is designated as a display, but on page 6 line 38 it is designated as a secure path.
3. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: The specification does not teach that the secure module is adapted to be "removably coupled to said personalized device" as stated in claim 12.

Appropriate correction is required.

### ***Claim Objections***

4. Claims 5 and 8 are objected to because of the following informalities: The word "favorable" is misspelled. Appropriate correction is required.

Art Unit: 2137

5. Claim 12 is objected to because of the following informalities: The specification does not teach that the secure module is adapted to be "removably coupled to said personalized device." Appropriate correction is required.

***Claim Rejections - 35 USC § 112***

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claim 6 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 6 recites the limitation "said output" in line 31. There is insufficient antecedent basis for this limitation in the claim.

***Claim Rejections - 35 USC § 102***

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Art Unit: 2137

9. Claims 1,2,4-12 are rejected under 35 U.S.C. 102(b) as being anticipated by Wang (US pat 5,917,913).

Regarding claim 1, Wang teaches a method of verifying data integrity between at least two correspondents in a public-key cryptographic scheme, at least one of said at least two correspondents having a main processor and a secure module, said secure module being independent of said main processor's control, said method comprising the steps of:

assembling data on at least one of said at least two correspondents (col.4 lines 12-17);

displaying data under control by said main processor to produce a first output (col.4 lines 17-21; col.2 lines 18-23),

displaying said data from said secure module to produce a second output (col.4 lines 41-44; col.10 line 66 thru col.11 line 5),

comparing said first output and second output (col.6 lines 35-48);

instructing said secure module to generate a signature upon a favorable comparison of said first output and said second output (col.4 lines 44-50; col.5 lines 50-67); and

whereby said favorable comparison indicates data integrity such that said at least one of said correspondents signs said data (col.4 lines 44-50; col.5 lines 50-67).

Regarding claim 2, Wang teaches at least one of said at least two correspondents is a personalized device (col.4 lines 8-12).

Regarding claim 4, Wang teaches said personalized device is a personal digital assistant (col.4 lines 8-12).

Regarding claim 5, Wang teaches said favorable comparison is characterized in that said first output and said second output are logically related to one another (col.6 lines 36-48).

Regarding claim 6, Wang teaches said logical relationship is such that said first output and said output are identical (col.6 lines 36-48).

Regarding claim 7, Wang teaches said step of displaying said data message includes displaying a portion of said data message (col.4 lines 41-44; col.10 line 66 thru col.11 line 5).

Regarding claim 8, Wang teaches said favorable comparison is characterized in that a portion of said first output and a portion of said second output are logically related to one another (col.6 lines 36-48).

Regarding claim 9, Wang teaches said logical relationship is such that said portion of said first output is identical to said portion of said second output (col.6 lines 36-48).

Regarding claim 10, Wang teaches a method of establishing a secure communication path for data between a personalized device and an user of said device in a PKI scheme, said device having a main processor and a secure module independently operative of said main processor, said method comprising the steps of:

providing all interface between said device and said user, said interface having an input device and an output device for providing a means for interaction between said user and device, said input device and output device controllable by said main processor (col.10 line 55 thru col.11 line 5);

providing a secure communication path between said secure module and a secure input device and a secure output device coupled thereto, said secure path logically isolated from any other communication path (col.6 lines 55-67);

comparing said data displayed on said output device and said secure output device (col.6 lines 36-48);

whereby said user of said personalized device can determine said integrity of said data based on said comparison (col.5 lines 18-21; col.5 lines 51-64; col.6 lines 36-48).

Regarding claim 11, Wang teaches said user actuates said secure input device based only on said output of said output device (col.6 lines 36-48).

Regarding claim 12, Wang teaches a method for verifying the integrity of a data message between a correspondent and a personalized device in a communication system, each correspondent adapted to receive and transmit data messages, said method comprising:

containing a secret key in said secure module, said secure module adapted to be removably coupled to said personalized device and communicatively coupled thereto (col.5 lines 1-9);



Art Unit: 2137

controlling access to said personalized device (col.11 lines 5-13).

***Claim Rejections - 35 USC § 103***

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wang, and further in view of Vatanen (WO 00/54457).

Regarding claim 3, Wang teaches the method of claim 2 but does not teach said personalized device is a mobile phone. Vatanen teaches said personalized device is a mobile phone (fig.1; page 7 lines 15-36). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Wang's portable electronic device with Vatanen's telecommunication system in order to implement a secure method for conducting transactions within a mobile telecommunication system (page 2 line 19 thru page 3 line 28).

**Conclusion**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tremayne M. Norris whose telephone number is (571) 272-3874. The examiner can normally be reached on M-F 7:30AM-5:00PM alternate Fridays.

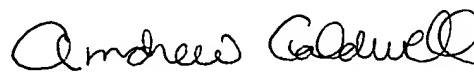
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Tremayne Norris

November 10, 2004



  
Andrew Caldwell